ENHANCED METHOD AND APPARATUS FOR DETECTING THE PRESENCE OF A WIRELESS NETWORK

RELATED APPLICATION

[0001] This application is a continuation-in-part of U.S. Application Serial No. 10/443,639, filed May 22, 2003, which, in turn, claims the benefit of U.S. Provisional Patent Application Serial No. 60/383,256 filed on May 24, 2002 both of which are incorporated herein by reference in their entirety.

BACKGROUND

[0002] The present invention, and the various embodiments thereof, relate to wireless network communications and, in particular, to the detection of a wireless computer network that is available to a mobile device user.

[0003] The demand for wireless communications has enjoyed tremendous growth over recent years and indeed, wireless communication technology is used every day by millions around the world to send, receive, and exchange information using pagers, cellular telephones, wireless personal digital assistants, and other wireless communication products. Recently, the revolution in wireless communication technologies has carried over to business and personal computing. Wireless communication technology now permits computer users to access and share information and data, without being tethered by wire to a computer network infrastructure traditionally used to connect computing devices.

[0004] The computer network infrastructure traditionally used to connect computing devices generally relies upon the implementation of standard local area network (LAN)

protocols, including Ethernet. These protocols permit organizations of every size to construct computer networks comprised of multiple computing devices connected to one another via hardwire connections. The traditional hardwired LAN provides for the high speed exchange of data using relatively inexpensive network connection devices. Indeed, a computer network is an essential requirement for operating a modern business enterprise. Employees of virtually every size business gain access to and share information and data over a digital LAN. Until recently, LANs required that the computing devices be interconnected using physical hardwired connections or network adapters forming the network infrastructure. Even computer users using portable laptop and notebook computers were relegated to having to connect these devices via a hardwired connection to the company infrastructure in order to gain access to the company network and its various resources, including data storage, modems, gateways, and printing devices.

[0005] The recent development and commercialization of wireless communications has now carried over to the corporate and indeed even the home LAN. Wireless network services offer great benefit to the mobile computer user. For example, the mobile user need not carry cumbersome cables and connectors to connect to a hard-wired network. Of course, the major benefit of a wireless LAN is the increased portability of computing devices used within such an infrastructure. Freed from the physical connections tying computing devices to the network, network users are free to move about the home or workplace without restriction, and are able to access a wireless LAN from nearly every location covered by the wireless network. On the other hand, wireless network services typically operate on unlicensed portions of the frequency spectrum where other potentially interfering and competing devices also operate.

[0006] A wireless LAN is typically implemented using radio transceivers which provide a wireless connection between the computing devices, or peripherals, and the network backbone comprised of other computers, servers, and peripherals. One or more transceivers are typically configured as wireless access points (WAPs). Wireless access points are, in turn, connected via a physical hardwire infrastructure to the computer network. The WAP further communicates via a radio link with radio transceivers associated with the computing devices of a user. Devices such as laptop or notebook computers, desktop computers, and even printers can be equipped with a wireless PC card, or wireless network adapter, containing the transceiver which communicates with the WAP.

[0007] Owing to the increased availability of wireless networks, laptop and notebook computer users are able to perform their tasks with increased mobility. For example, a user can take his or her laptop from their desk into a conference room to attend a meeting and still have access to the network to retrieve data and have access to the Internet via one or more modems or gateways present on the network -- all without being tethered by a wired connection. Similarly, mobile computer users and business travelers commonly use their portable computers to gain access to their email accounts, to determine if there is any unread email, and to read and send email. Still further, being able to connect to the Internet permits the user to perform these tasks and others without having to suffer through the lackluster performance provided by conventional 56K modem connections which use the telephone network to establish communications. Indeed, high speed Internet access via a WAP is highly desirable when considered vis-a-vis a connection made via use of a conventional 56K modem. Thus, as more and more laptop and notebook computers are being equipped with integrated wireless network adapters, the implementation of wireless LANs in the business environment, and even within residences, is surely to expand.

[0008] A further expansion of the use of wireless computer networks now permits laptop and notebook computer users to use their portable computing devices to access public and private computer networks at locations away from their own office or home networks. Internet service providers, telecommunications companies, and wireless network providers have begun to install WAPs in locations such as airport lounges, hotel lobbies, and coffee bars. WAPs are being established at these and other public locations where business travelers and general computer users often congregate. These types of public WAPs are typically referred to as "hotspots." A typical hotspot permits a wireless computer user to gain access to a computer network via a wireless connection created between the wireless network adapter in the user's computer and the public WAP. The hotspot WAP permits the user to gain access to an IP address associated with a modem or gateway to enable the computer user to access the Internet and, potentially, other local network resources, such as printers, which are associated with the hotspot.

[0009] Public access points may be associated with "open networks" as well as "closed networks." An open network, for purposes of this disclosure, is a network associated with a public WAP which is accessible to computer users without the need to have previously subscribed to the network operated by the WAP provider. A closed network, for purposes of this disclosure, is a network associated with a public WAP which is accessible to computer users who are already registered users of the network and who, in all likelihood, have paid a fee for such access. A closed network will typically present the user with a login screen, procedure, or script, which may require the user to provide a user name and password to gain access to the network associated with the WAP. An open network may not require any formal login.

[00010] In practice, a mobile computer user, such as business traveler carrying a notebook computer, may come upon an airport waiting area or hotel lobby equipped with a WAP. While printed signs may advertise the presence of a WAP, the user has no idea whether the network is indeed active, whether the wireless signal extends to where the user is sitting, or whether the signal strength is adequate to permit a reliable connection to be made with the network. Thus, to attempt to connect to a network via a WAP, the mobile computer user is required to unpack their computer, turn the computer on, wait for it to boot, perform any necessary network configuration, and thereafter launch a web browser before they are able to determine if it is indeed possible to gain access to the network via the WAP, let alone browse the Internet or check for the presence of unread email. As will be appreciated, these steps are found to be very time consuming and frustrating for consumers, especially when it is determined that the WAP fails to exist or is not capable of providing adequate network access.

SUMMARY

[00011] To provide a more convenient means for accessing a wireless network, the following describes examples of systems and methods for detecting the presence of a computer network. In this regard, the systems and methods described hereinafter may be used in connection with a wireless communication apparatus which indicates to a computer user the existence of a wireless computer network without requiring use of their computer. In addition, the systems and methods described hereinafter may be utilized in connection with a portable handheld wireless communication device which permits a mobile computer user to gain access to a wireless LAN and determine whether unread email is present, all without the need of booting one's laptop computer. Still further, the systems and methods described hereinafter may be used

in connection with a portable wireless device which is capable of identifying and/or displaying the public and private wireless networks which are available at a given location.

[00012] A better understanding of the objects, advantages, features, properties and relationships of such exemplary embodiments will be obtained from the following detailed description and accompanying drawings which further demonstrate the various ways in which the principles of the subject systems and methods may be employed.

BRIEF DESCRIPTION OF THE DRAWINGS

[00013] For a better understanding of the exemplary systems and methods for detecting the presence of a computer network which are described hereinafter, reference may be had to preferred embodiments shown in the following drawings in which:

[00014] Figure 1 illustrates a block diagram representation of an exemplary system for use in determining the presence of a wireless network;

[00015] Figure 2 illustrates the system of Figure 1 embodied in a first handheld device;

[00016] Figure 3 illustrates the system of Figure 1 embodied in a second handheld device;

[00017] Figure 4 illustrates an exemplary 802.11 frequency spectrum;

[00018] Figure 5 illustrates a block diagram representation of a further exemplary system for use in determining the presence of a wireless network and for communicating with the wireless network;

[00019] Figure 6 illustrates the system of Figure 5 embodied in a third handheld device;

[00020] Figure 7 illustrates a block diagram of software layers within the system of Figure 5; and

[00021] Figure 8 illustrates an exemplary schematic diagram representation of the system of Figure 1.

[00022] Figure 9 illustrates an exemplary schematic diagram representation of a further embodiment of the present invention.

DETAILED DESCRIPTION

[00023] Turning now to the figures, wherein like reference numerals refer to like elements, exemplary systems and methods for detecting the presence of a computer network are

hereinafter described. To this end, Fig. 1 illustrates a block diagram representation of an exemplary system 10 which functions as a passive detector for purposes of determining the presence of a wireless network. In the illustrative example, the system 10 includes a microprocessor 11 that operates in conjunction with a radio receiver 12 to determine the presence of a wireless network and, in particular, to discriminate between a wireless computer network implementing the 802.11 protocols (e.g., 801.11b a.k.a. WiFi and 802.11a a.k.a. WiFi5) and other in-band non-network sources of radio frequency energy and sources of radio frequency interference such as microwave ovens, Bluetooth devices and 2.4 GHz cordless telephones. As will be appreciated, the radio receiver 12 operates under the control of the microprocessor 11, via a bus 13, and the microprocessor 11 may comprise one of the class of microprocessor devices which incorporate onboard logic as well as a ROM and/or RAM in which instructions for controlling the operation of the system could be stored. By way of further example, Fig. 8 illustrates a schematic diagram of the system 10 wherein receiver 12, connected via socket J1, is radio transceiver chip type Micro Linear ML2725 in which only the receiver is used. Fig. 9 illustrates a schematic diagram of a further embodiment of the present invention.

[00024] For use in detecting the presence of a computer network, the microprocessor 11 preferably includes instructions for causing the receiver 12 to scan the frequency bands utilized in implementing 802.11 wireless networks as described hereinafter in connection with Fig. 4. Scanning of the frequency bands by the receiver 12 may be made possible through use of an antenna 15 that is connected to the receiver 12. The antenna 15 allows the receiver 12 to receive ambient radio signal in response to which the receiver 12 outputs a Received Signal Strength Indication (RSSI) signal. The RSSI signal may then be supplied to an analog-to-digital converter

input port on the microprocessor 11 via, for example, a communication line 14 that links the receiver 12 to the analog-to-digital converter input port.

[00025] To cause the system 10 to scan the frequency bands, the mobile computer user may depress a switch 19 which causes the software program stored within microprocessor 11 to execute. The microprocessor 11 would then drive receiver 12 causing it to scan the various 802.11 frequencies and to measure the energy of any received signals within the relevant band. A signal indicative of the signal strengths are, in turn, provided to the microprocessor 11 where the information is used to discriminate between an 802.11 wireless computer network and devices such as, for example, microwave ovens and cordless phones.

[00026] To provide for ease of use, the above-described system 10 may be embodied in a handheld device 10 having a single switch 19 and single LED 16 connected to a power supply 18 via means of a resistor 17 as is illustrated in Figs. 1 and 2. While not required, it will be appreciated that the LED 16 can comprise a tri-colored LED, where the LED glows red to indicate that a wireless network has not been detected, yellow to indicate that a wireless network may be present and green to indicate that indeed a wireless network has been detected as being present. Such a tri-colored LED 16 would be driven by the microprocessor 11 according to its programming and as a function of the signal(s) received from the receiver 12.

[00027] Alternatively, the above-described system 10 may be embodied in a handheld device 30 having a single switch 19 accompanied by a multi-segment display 20 comprising a plurality of LEDs as is illustrated in Fig. 3. In this illustrated embodiment, the number of LEDs illuminated may correspond to the relative received signal strength as measured by the system towards providing the user with further information as to the perceived strength of the signal associated with the detected wireless computer network. Again, the display 20 would be driven

by the microprocessor 11 according to its programming and as a function of the signal(s) received from the receiver 12. It will also be appreciated that an analog meter, illuminating LCD segments, etc. can be used for this same purpose.

[00028] Thus, through use of the systems illustrated in Figs. 1-3, it will be seen that a mobile computer user can easily verify the presence of a wireless computer network without having to ever turn on their computer.

[00029] To determine the presence of a wireless computer network, the software associated with the microprocessor 11 may cause the receiver 12 to scan the relevant 802.11 frequency band and receive the ambient radio signal and generate a received signal strength indication. To this end, the system may operate to initially scan just outside of the 802.11 band looking at the noise outside the band in an attempt to identify the energy level "out-of-band." If the measured signal energy out-of-band is significant, it can be concluded that the received signal is most likely emanating from a microwave oven or other broadband sources, inasmuch as a microwave oven or these sources when operating may spread a great deal of "noise" across a wide band spectrum. For example, software resident in microprocessor 11 may cause the receiver 12 to scan the 802.11 B frequency band starting somewhat low, outside of the band "L," and ending high, outside of the band "U."

[00030] The overall frequency band could also be scanned in 2 MHz steps, 41 – 45 as illustrated in Fig. 4, where the results are integrated over time such that the overall energy level of the band may be measured. If the software associated with the microprocessor 11 determines that the energy level is somewhat constant over time, and that the energy level exceeds a predefined threshold, the signal received by the receiver 12 may be deemed to be that emanating from an 802.11 wireless network. In this regard, it is to be appreciated that 802.11b transceivers

will typically keep transmitting short bursts of data and then switch to a receive mode. However, it can be expected that the frequency of the bursts will be contained within one 802.11b channel. Thus, if the peak energy level is detected as moving and/or the overall energy level is fluctuating and/or appearing and disappearing, it can be assumed that the received signal is not emanating from a wireless network but instead emanating some noise generating electronic device such as a microwave oven, Bluetooth or cordless phone source. Bluetooth and other Frequency Hopping Spread Spectrum ("FHSS") schemes would be "jumpy" in frequency as well as time. Indeed, a microwave oven when operating spreads a great deal of "noise" across a wide band spectrum in intermittent short bursts of energy, i.e., microwave ovens are pulsed at 60Hz, and its energy would appear in every channel at 1/60 seconds which is easy to detect. On the other hand, a cordless telephone typically operates by remaining on much longer and with a higher duty cycle. Analog cordless telephones can be recognized right away by detecting a constant carrier thereby discriminating wireless cameras and inexpensive cordless phones. Similarly, since digital cordless telephones can operate using a FHSS or Direct Sequence Spread Spectrum ("DSSS") scheme, telephones using these schemes can be identified by their duty cycle. A cordless telephone utilizing a FHSS scheme can be spotted by the appearance of signals in several 802.11b channels. While DSSS telephones can be more difficult to recognize, since some DSSS telephones transmit over long periods of time, such telephones can be detected by analyzing the duty cycle of the detected signal. The characteristics of a wireless network can thus be detected by the system and its existence discriminated from other radio frequency sources operating within the same band as a 802.11 wireless network.

[00031] Beacon signals that are periodically transmitted from an access point may also be utilized to discern the presence or absence of an 802.11 wireless network. In this regard, since

the 802.11 specification provides for a client to roam among multiple access points that can be operating on the same or separate channels, the 802.11 specification requires the periodic transmission of beacon signals. Although the 802.11 specification does not mandate the rate of transmission or the specific contents of the beacon signal (only requiring that the established period be maintained), by popular convention the beacon signal is generally transmitted periodically at a rate of every 100 ms and generally includes a time stamp for client synchronization, a traffic indication map, an indication of supported data rates, and other parameters. This rate and information has been found sufficient for the purpose of allowing roaming clients to gauge the strength of their existing connection to an access point and, if the connection is judged weak, to associate itself with a new access point.

[00032] More particularly, the presence or absence of an 802.11 wireless network may be discerned by having software associated with the microprocessor 11 look for patterns in the RSSI that are indicative of beacon transmissions. To this end, the system may detect the presence of beacon signals by looking for the presence of energy in a pattern consistent with the expectations of a beacon signal, as generally described above. For example, when the system detects a pulse having a duration between an established minimum and maximum, e.g., a range sufficient to transmit a time stamp for client synchronization, a traffic indication map, an indication of supported data rates, and other parameters, the system stores information representative of the timing of the detected pulse. Thus, if other pulses are detected with an appropriate periodicity, e.g., at a rate of approximately 100 ms, it can be determined that the detected pulses are beacon pulses originating from a 802.11 wireless access point and, as such, a 802.11 wireless network is present.

[00033] It will be appreciated that this method for determining the presence or absence of a 802.11 wireless network does not rely upon scanning. Rather, the system can receive the entire band all at once. All measurements can then be done directly without the need to compare energies of multiple "channels." While signals from interfering devices cannot be discriminated by frequency using this method alone, the failure of such devices to transmit signals having the duration and the periodicity of the beacon signal is sufficient to allow the system to determine whether any received signals are originating from an 802.11 wireless network access point or from another device. It will be additionally appreciated that constant, narrow band interferers such as analog cordless phones will just add an offset to the overall energy level and, therefore, will not have any real effect, positive or negative, on the ability of this method to detect a WLAN signal.

[00034] An alternative system 50 that provides enhanced functionality to the user by operating not only as a passive device capable of identifying the presence of a wireless computer network, but also as an active device able to affirmatively interrogate or otherwise communicate with a wireless computer network, as well as communicate with the Internet towards carrying out a variety of functions, is illustrated in Fig. 5. For performing these functions, the system illustrated in Fig. 5 comprises a microprocessor 51 which is in communication, via bus 54, with a transceiver 52 linked to an antenna 53. In this illustrated example, the transceiver 52 may comprise, for example, an Intersil PRISM-II integrated circuit based transceiver. As in the system described previously with respect to Fig. 1, a received signal strength indication (RSSI) is generated by transceiver 52 on line 55 which is input to microprocessor 51 and its on board analog-to-digital converter. However, while the system of Fig. 5 can make use of the RSSI signal, this system is distinguished from the system illustrated in Fig. 1 by its ability to provide

bi-directional data communication from the transceiver 52. Thus, due to the increased sophistication of this system, a more powerful microprocessor may be used and is shown in Fig. 5 as including EEPROM 60 and I/O 61 driving a Universal Serial Bus ("USB") connection 62.

[00035] For convenience of use, the system of Fig. 5 may be embodied in a handheld device 70 as is illustrated in Fig. 6. As illustrated in Fig. 6, the handheld device 70 may include a plurality of switches 58, 59, and 63 linked to the microprocessor 51. As previously described in connection with Fig. 1, one switch, e.g., 58, could be activated to cause the system to determine if a wireless network is present. Possible uses for switches 59 and 63, as well as an alpha-numeric display 56 which is under the control of the microprocessor 51, will be described below.

[00036] In operation, the system 50 can communicate bi-directionally with a wireless network and indeed other computers and servers accessible over the network and can, in turn, provide the user with enhanced functions that can be carried out all without ever turning on a computer. By way of example, the system 50 can serve to permit the user to actually issue a "ping" command to the network, for example, by activating switch 63. As illustrated in Fig. 7, the system architecture includes all the necessary components to execute such commands. By issuing a "ping" command, the user will cause the system 50 to attempt to establish contact with a computer server located outside of the network, operated by the wireless computer access point provider. A user may "ping" a known IP address corresponding to, for example, a familiar web site such as "yahoo.com." The "ping" command may or may not generate a response. Receiving a positive response to a "ping" command can serve to indicate to the user that the network is open and permit the user to have free access to the Internet and not just a server associated with the WAP operator's own site. The display 56 may be used to provide the user with information

concerning the positive response. The particular Internet address configured for the automated "ping" operation can optionally be configured by interfacing with a personal computer via USB port 62 or in another embodiment, can optionally be configured wirelessly. By configuring the ping address to the user's own email server or corporate intranet login server, the user is able to confirm access to a specific desirable address.

[00037] Still further, the system 50 may be utilized to provide a much more powerful function whereby a user can determine whether or not the user has unread email in an appropriate email account -- all without having to utilize their laptop or notebook computer. In operation, the user would merely press and hold, for example, the email button 59 on the device 50 to initiate a command sequence. Software resident on the system will cause microprocessor 51 to command the transceiver 52 to attempt to access the wireless computer network. Given the system architecture, the device can further be commanded to interrogate a POP3 email server to detect whether the user has any unread email and can receive an appropriate response and provide an indication to the user on display 56 stating, for example, that "the user has 7 unread messages." Yet further, the system 50 may be utilized to permit the mobile user to determine if anyone has attempted to "instant message" the user.

[00038] For retrieving email or "instant message" information, the system 50 would be configured to know the identity of the user and their POP3 server(s) and possibly other security parameters, all of which can be provided to the device via I/O 61 and USB connection 62. Using USB connection 62, the device can be connected to a PC which can permit the user to configure the system 50 with any information needed to access such accounts. USB port 62 can also be used to download other software commands necessary to make the system 50 compatible with

the networks and/or servers to be accessed and to generally operate as intended. It is to be appreciated that the configuration of the system 50 can also be accomplished wirelessly.

[00039] From the foregoing, it will be understood that one very attractive use of the system 50 is the distribution of pre-configured devices by an email service operator and/or access point operator. Such an entity could distribute pre-configured/pre-programmed devices including the system 50 to its email account holders. Users in turn could then determine if they had unread mail thereby generating additional traffic to the service operator. Such devices could further be pre-configured to have limited functionality, for example, a device that permits the user to detect whether or not unread email exists on one and only one account, namely that associated with the entity issuing the device.

[00040] In the case of closed networks, the system 50 can be configured to transmit to the WAP the various protocols required for the user to log onto the network. The system 50 could listen for the appropriate response from the WAP, identify the network and determine indeed whether or not they are able to log onto the network and if so, ask to issue an appropriate predefined encryption key and/or password to the device to permit access to the network and its resources. The user can then use the system 50 to download the network set-up command to their computer via, for example, the USB connection 62. Thus, the system 50 can be configured to be operational with multiple networks, as well as provide an indication as to how strong the signal strength emanating from the access point is and other system parameters.

[00041] A limited purpose device including the system 50 could be provided which is populated with a single encryption key that limits use of the device to a single network and or limits the functionality of the device on the network that has multiple tiers of services. For example, the present apparatus could be configured to permit users to have trial access to a

closed wireless network by setting up the various required authentications and other passwords. The device can be designed to have as much or as little functionality as the WAP provider/operator and/or wireless computer network operator so desires.

[00042] While various concepts have been described in detail, it will be appreciated by those skilled in the art that various modifications and alternatives to those concepts could be developed in light of the overall teachings of the disclosure. As such, the particular concepts disclosed are meant to be illustrative only and not limiting as to the scope of the invention which is to be given the full breadth of the appended claims and any equivalents thereof.